

EUROPEAN PATENT OFFICE

Patent Abstracts of Japan

PUBLICATION NUMBER : 08272742
 PUBLICATION DATE : 18-10-96

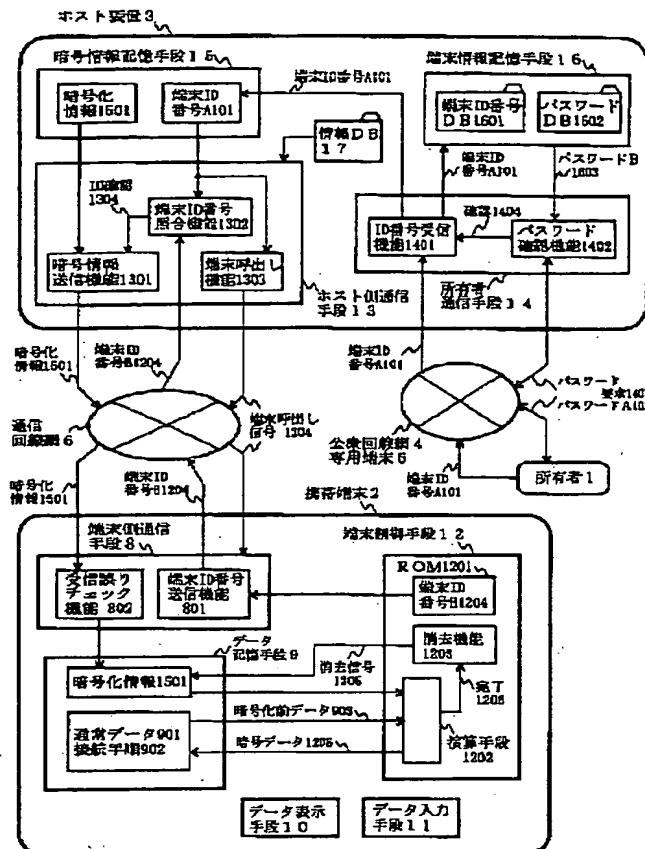
APPLICATION DATE : 30-03-95
 APPLICATION NUMBER : 07072781

APPLICANT : HITACHI LTD;

INVENTOR : SHIMIZU HIROSHI;

INT.CL. : G06F 15/00 G09C 1/00 H04L 9/32

TITLE : DATA LEAK PREVENTION SYSTEM



ABSTRACT : PURPOSE: To prevent data from leaking when a portable terminal is lost or stolen by ciphering internal stored data with ciphering information sent from a host device and deleting the ciphering information at the end of the ciphering.

CONSTITUTION: When the owner 1 becomes aware that the portable terminal 2 is lost and performs data leak preventing operation through public telephone line 4, an owner communication means 14 of the host device 3 receives the terminal ID number, a terminal information storage means 16 takes the password out on the basis of the terminal ID number, and a password confirming function 1402 confirms whether the password that the owner has inputted matches with the taken-out password. When their coincidence is confirmed, a cipher information transmitting function 1301 sends the cipher information, stored in a cipher information storage means 15, to the terminal 2. A terminal control means 12 of the terminal 2 ciphers normal data and a connection procedure stored in a data storage means 9 according to the ciphering information and after the ciphering ends, an erasing function 1203 generates an erasure signal to erases the ciphering information stored in the data storage means 9.

COPYRIGHT: (C)1996,JPO

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開平8-272742

(43)公開日 平成8年(1996)10月18日

(51)Int.Cl.⁶
G 0 6 F 15/00
G 0 9 C 1/00
H 0 4 L 9/32

識別記号 330
9364-5L
7259-5J

F I
G 0 6 F 15/00
G 0 9 C 1/00
H 0 4 L 9/00

技術表示箇所
330C
A

審査請求 未請求 請求項の数9 OL (全19頁)

(21)出願番号 特願平7-72781

(22)出願日 平成7年(1995)3月30日

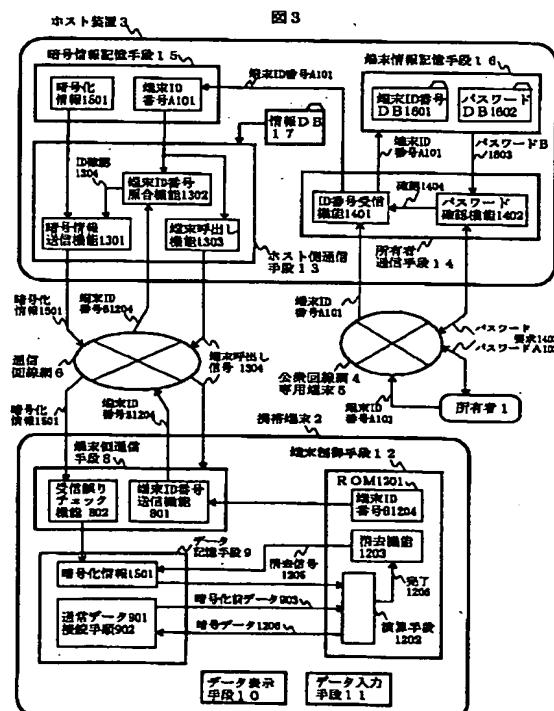
(71)出願人 000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目6番地
(72)発明者 横沢 達
神奈川県横浜市戸塚区吉田町292番地株式
会社日立製作所映像メディア研究所内
(72)発明者 清水 宏
神奈川県横浜市戸塚区吉田町292番地株式
会社日立製作所映像メディア研究所内
(74)代理人 弁理士 小川 勝男

(54)【発明の名称】 データ漏洩防止システム

(57)【要約】

【構成】データを暗号化する演算手段1202と、データを記憶するデータ記憶手段9と公衆回線や一般加入回線を介して所有者と通信を行う所有者通信手段14と、その所有者が入力する端末ID番号と端末側での暗号化に使用する暗号化情報を記憶する暗号情報記憶手段15と、暗号化情報を携帯端末へ送信するホスト側通信手段13とを有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段9と、ホスト装置と通信をする機能を持つ端末側通信手段8と、暗号化情報を消去する機能1203と、暗号化処理をするための演算手段を有する携帯端末を設ける。

【効果】携帯端末の所有者は端末の紛失や盗難に伴うデータ漏洩を最小限にとどめることができる。



【特許請求の範囲】

【請求項1】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力する為のデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、公衆回線網または専用端末を介して前記携帯端末の所有者と通信を行うための所有者通信手段と、前記所有者通信手段により入力される情報と、暗号化に必要な暗号化情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段と、前記携帯端末に各種の情報を提供する為のデータを蓄積した情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、

前記携帯端末がデータ記憶手段に通常のデータ以外にホスト装置から送信された暗号化情報と、端末からホスト装置を呼出す為の接続手順を記憶する機能、端末制御手段に前記暗号化情報を消去する機能、前記読み出し専用記憶手段に前記端末である事を示す為の端末ID番号を記憶する機能、前記演算手段に前記暗号化情報により前記データ記憶手段に記憶されたデータを暗号化する機能、端末側通信手段にホスト装置との通信を開始するときに端末ID番号を送信する機能と、暗号化情報を受信して受信誤りをチェックし、データ記憶手段へ入力する機能を備え、前記ホスト装置が端末情報記憶手段に各端末につけられた端末ID番号と前記端末の所有者へのパスワードを記憶する機能、所有者通信手段に回線網または専用端末を介して所有者が入力する端末ID番号を受信する機能と、端末情報記憶手段から端末ID番号を元にパスワードを取り出し、本人からの通信であることを前記パスワードにより確認する機能と、前記確認された端末ID番号を前記暗号情報記憶手段に登録する機能、ホスト側通信手段に前記暗号情報記憶手段に記憶された端末ID番号と、端末から通信回線網を介して送信された端末ID番号を照合し、登録された携帯端末との通信であることを検出する機能と、端末ID番号により前記番号の端末を呼出す機能と、前記暗号情報記憶手段から取り出した暗号化情報を携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化するために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ID番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが

確認されると、前記端末ID番号が暗号化を行う端末として暗号情報記憶手段に登録され、この後、通信回線網を介して携帯端末が前記接続手順を用いるか、またはホスト装置が前記端末の端末ID番号を用いて通信が開始され、携帯端末からホスト装置へ端末ID番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、暗号情報記憶手段から暗号化情報がホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記暗号化情報は受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記暗号化情報を用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号化情報を消去して、暗号を解くための情報を端末内から無くすことで、携帯端末が手元に無い場合でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項2】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力する為のデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、公衆回線網または専用端末を介して前記携帯端末の所有者と通信を行うための所有者通信手段と、前記所有者通信手段により入力される情報と、復号化に必要な復号化情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段と、前記携帯端末に各種の情報を提供する為のデータを蓄積した情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、前記携帯端末がデータ記憶手段に通常のデータ以外にホスト装置から送信された復号化情報を記憶する機能、前記読み出し専用記憶手段に前記携帯端末である事を示す為の端末ID番号を記憶する機能、前記演算手段に前記復号化情報をにより前記データ記憶手段に記憶された暗号化済みデータを復号化する機能、端末側通信手段にホスト装置からの呼出しに対して前記端末ID番号を受信応答として送信する機能と、復号化情報を受信して受信誤りをチェックし、データ記憶手段へ入力する機能を備え、また、前記ホスト装置が端末情報記憶手段に各端末につけられた端

末ID番号と前記端末の所有者へのパスワードを記憶する機能、所有者通信手段に回線網または専用端末を介して所有者が入力する端末ID番号を受信する機能と、端末情報記憶手段から端末ID番号を元にパスワードを取り出し、本人からの依頼であることを前記パスワードにより確認する機能と、前記確認された端末ID番号をホスト側通信手段に入力する機能、ホスト側通信手段に公衆回線網を介して入力された端末ID番号で携帯端末を呼出す機能と、前記携帯端末が受信応答として送信した端末ID番号により接続を確認する機能と、前記暗号情報記憶手段の復号化情報を読み出して前記携帯端末へ送信する機能を備えることで、既に前記携帯端末のデータ記憶手段のデータが暗号化された状態で、所有者が前記データを復号化するために、所有者が最寄りの電話機または専用端末により前記携帯端末のホスト装置に接続し、端末ID番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力した前記パスワードが確認されると、前記端末ID番号は復号化を指定された端末としてホスト側通信手段へ入力され、通信回線網を介して端末の呼出しが行われ、ホスト側通信手段が端末側から端末ID番号で応答を受けて通信が確立されると、ホスト側通信手段により暗号情報記憶手段の復号化情報が通信回線網を介して端末へ送信され、一方、端末側通信手段が受信した復号化情報は前記データ記憶手段に記憶され、演算手段が前記復号化情報を用いてデータ記憶手段のデータを復号化することで、復号化の為の情報をデータ記憶手段に記憶していない携帯端末でも、通信回線網を介して前記データ記憶手段に記憶された暗号データを参照可能なデータに変換できる事を特徴とするデータ漏洩防止システム。

【請求項3】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力するためのデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、公衆回線網または専用端末を介して前記携帯端末の所有者と通信を行うための所有者通信手段と、前記所有者通信手段により入力される情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段と、前記携帯端末に各種の情報を提供する為のデータを蓄積した情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、前記携帯端末がデータ記憶手段に通常のデー

タ以外に暗号化と復号化の為の暗号化情報を記憶する機能と、端末からホスト装置を呼出す為の接続手順を記憶する機能、端末制御手段に前記暗号化情報を端末側通信手段を介して外部より受信するコマンドにより消去できる機能、前記読み出し専用記憶手段に前記端末である事を示す為の端末ID番号を記憶する機能、前記演算手段に日常動作においてデータ記憶手段の内の暗号化情報以外のデータを常に暗号化する機能と、必要なときのみ暗号化済みのデータを復号化する機能、端末側通信手段にホスト装置との通信を開始するときに端末ID番号を送信する機能と、ホスト装置から通信回線網を介して送信される暗号化情報の消去コマンドを受信する機能を備え、また、前記ホスト装置が端末情報記憶手段に各端末につけられた端末ID番号と前記端末の所有者へのパスワードを記憶する機能、所有者通信手段に回線網または専用端末を介して前記端末ID番号が入力されると、端末情報記憶手段から端末ID番号を元にパスワードを取り出し、本人からの通信であることを前記パスワードにより確認する機能と、前記確認された端末ID番号を暗号情報記憶手段に登録する機能、ホスト側通信手段に通信回線網を介して端末ID番号で端末を呼出す機能と、前記暗号情報記憶手段に記憶された端末ID番号と端末から送信された端末ID番号を照合し、登録された携帯端末との通信であることを検出する機能と、前記検出により前記暗号情報記憶手段から取り出した前記暗号化情報を消去するコマンドを、携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末のデータ復号化機能を無効にするために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ID番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ID番号が復号化機能を無効にする端末として暗号情報記憶手段に記憶され、この後、携帯端末が前記接続手順を用いるか、またはホスト装置が前記端末の端末ID番号を用いて通信を開始して、携帯端末からホスト装置へ端末ID番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、前記暗号化情報を消去するコマンドが前記携帯端末へ送信され、前記消去コマンドを受信した携帯端末が、端末制御手段により前記データ記憶手段内の暗号化情報を消去して復号化機能を無効にすることで、携帯端末が手元に無い場合でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項4】請求項1において、前記暗号化情報を暗号化プログラムと暗号キーとし、前記携帯端末の演算手段

に前記暗号化プログラムを実行し、前記暗号キーに基づいて前記データ記憶手段に記憶された前記暗号化情報を除くデータを暗号化する機能、前記端末制御手段に暗号化プログラムと暗号キーを消去する機能、端末側通信手段に前記暗号キーと暗号化プログラムを暗号情報として受信して前記データ記憶手段へ入力する機能、また前記ホスト装置が暗号情報記憶手段に暗号化情報として暗号化プログラムと暗号キーを予め記憶する機能、ホスト側通信手段に暗号情報記憶手段から取り出した暗号化プログラムと暗号キーを携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータを暗号化するために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ID番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ID番号が暗号化する端末として暗号情報記憶手段に登録され、この後、携帯端末が前記接続手順を用いて、またはホスト装置が前記端末の端末ID番号を用いて通信が開始され、携帯端末からホスト装置へ端末ID番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、暗号情報記憶手段から暗号化プログラムと暗号キーがホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記暗号化プログラムと暗号キーは受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記暗号化プログラムと暗号キーを用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号化プログラムと暗号キーを消去して、暗号を解くための情報を端末内から無くすることで、携帯端末が手元に無く、さらに暗号化の為のプログラムも内蔵していない携帯端末でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項5】請求項1において、前記暗号化情報を暗号キーと制御コマンドとし、前記携帯端末が前記読み出し専用記憶手段に予めプログラムを記憶し、前記演算手段に前記制御コマンドに従って前記プログラムを実行し、前記暗号キーにより前記データ記憶手段に記憶されたデータを暗号化する機能、前記端末制御手段に暗号キーを消去する機能、端末側通信手段に前記暗号キーと制御コマンドを暗号情報として受信し、前記暗号キーは前記データ記憶手段へ、前記制御コマンドは前記端末制御手段へ入力する機能、また前記ホスト装置が暗号情報記憶手段に暗号化情報として制御コマンドと暗号キーを予め記憶する機能、ホスト側通信手段に前記暗号情報記憶手段から取り出した制御コマンドと暗号キーを携帯端末へ送

信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化をするために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ID番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ID番号が暗号化を行う端末として暗号情報記憶手段に登録され、この後、携帯端末が前記接続手順を用いて、またはホスト装置が前記端末の端末ID番号を用いて通信が開始され、携帯端末からホスト装置へ端末ID番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確認され、前記端末である場合には、暗号情報記憶手段から制御コマンドと暗号キーがホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記制御コマンドと暗号キーは受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記制御コマンドと暗号キーを用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号キーを消去して、暗号を解くための情報を端末内から無くすることで、携帯端末が手元に無くても、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項6】請求項1において、前記暗号化情報を暗号化プログラムとし、前記携帯端末が前記読み出し専用記憶手段に予め暗号キーを記憶し、前記演算手段に前記暗号化プログラムに従って前記プログラムを実行し、前記暗号キーにより前記データ記憶手段に記憶されたデータを暗号化する機能、前記端末制御手段に暗号化プログラムを消去する機能、端末側通信手段に前記暗号化プログラムを暗号情報として受信し、前記データ記憶手段へ入力する機能、また前記ホスト装置が暗号情報記憶手段に暗号化情報として暗号化プログラムを予め記憶する機能、ホスト側通信手段に前記暗号情報記憶手段から取り出した暗号化プログラムを携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化をするために、最寄りの電話機または専用端末より前記携帯端末のホスト装置に接続し、端末ID番号を入力すると、所有者通信手段によりパスワードを要求され、所有者が入力したパスワードが確認されると、前記端末ID番号が暗号化を行う端末として暗号情報記憶手段に登録され、この後、携帯端末が通信回線網を介して前記接続手順を用いるか、またはホスト装置が前記端末の端末ID番号を用いて通信が開始され、携帯端末からホスト装置へ端末ID番号が送信されると、ホスト側通信手段により前記暗号情報記憶手段に登録されている携帯端末との通信であるか否かが確

認められ、前記端末である場合には、暗号情報記憶手段から暗号化プログラムがホスト側通信手段を介して前記携帯端末へ送信され、一方、端末側通信手段に受信された前記暗号化プログラムは受信誤りをチェックされた後、前記データ記憶手段に記憶され、前記演算手段が前記プログラムと暗号キーを用いてデータ記憶手段のデータの暗号化を行い、端末制御手段が暗号化の完了と共に前記暗号化プログラムを消去して、暗号を解くための情報を端末内から無くすことで、携帯端末が手元に無く、さらに暗号化の為のプログラムも内蔵していない携帯端末でも、通信回線網を介して前記端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項7】ホスト装置と通信回線網を介してデータ送受信をする為の端末側通信手段と、書換えが可能でかつ一旦記憶操作が行われた後は、外部からの給電無しに各種データを保持できるデータ記憶手段と、前記データ記憶手段に保持されたデータを所有者に提示するためのデータ表示手段と、所有者がデータを入力するためのデータ入力手段と、前記端末側通信手段とデータ記憶手段とデータ表示手段とデータ入力手段を制御する端末制御手段と、前記端末制御手段に一度だけ書き込みが出来る読み出し専用記憶手段と演算手段を備え、手軽に携行できる携帯端末、および、前記携帯端末と通信回線網を介してデータ送受信をする為のホスト側通信手段と、復号化に必要な復号化情報を保存する為の暗号情報記憶手段と、前記携帯端末に関する情報を記憶する端末情報記憶手段とを有した前記携帯端末のホスト装置よりなる携帯端末を用いたデータ通信システムであって、前記携帯端末がデータ記憶手段に通常のデータと所有者がデータ入力手段から入力する暗号化情報と、端末からホスト装置を呼出す為の接続手順を記憶する機能、端末制御手段に後述する暗号化要求を受けると、暗号化で使用する暗号化情報の入力を前記データ表示手段を介して所有者に要求する機能と、前記暗号化情報の入力により暗号化開始指示を端末側通信手段に入力する機能と、前記暗号化情報を消去する機能、前記読み出し専用記憶手段に前記端末である事を示す為の端末ID番号を記憶する機能、前記演算手段に前記暗号化情報により前記データ記憶手段のデータを暗号化する機能と、前記暗号化を後述する送信終了により開始する機能、データ入力手段に所有者が暗号化要求を前記端末制御手段に入力する機能と、前記暗号化情報を前記データ記憶手段に入力する機能、端末側通信手段に暗号化開始指示を受けると前記接続手順でホスト装置と接続する為に端末ID番号を送信する機能と、前記暗号化情報を復号化情報として前記ホスト装置へ送信する機能と、前記復号化情報をホスト装置へ送信した事を前記演算手段に送信終了により通知する機能を

備え、また、前記ホスト装置が端末情報記憶手段に予め登録された各端末の端末ID番号を記憶する機能、ホスト側通信手段に前記端末情報記憶手段に記憶された端末ID番号と端末から送信された端末ID番号を照合し、登録された携帯端末との通信であることを検出する機能と、前記照合された端末ID番号を前記暗号情報記憶手段に登録する機能と、受信した前記復号化情報を前記照合された端末ID番号と共に前記暗号情報記憶手段に記憶する機能を備えることで、携帯端末の所有者が何らかの事情により、前記端末内のデータの暗号化をするために、暗号化要求指示を前記データ入力手段より入力すると、前記データ表示手段を介して前記端末制御手段から暗号化情報の入力を要求され、所有者が前記要求に従つて前記データ入力手段から暗号化情報を入力すると、前記暗号化情報が前記データ記憶手段に記憶され、これにより端末制御手段から暗号化開始指示が前記端末側通信手段に入力され、前記通信手段が前記接続手順により通信回線網を介して前記ホスト装置を呼出し、接続すると端末ID番号と復号化情報が送信され、一方、呼出しを受けたホスト装置ではホスト側通信手段により端末ID番号が照合され、検出された前記端末ID番号は続いて受信される復号化情報暗号と共に暗号情報記憶手段に記憶され、次いで、前記端末側通信手段が送信終了を前記演算手段に入力すると、前記演算手段が前記暗号化情報を用いて前記データ記憶手段にあるデータの暗号化を開始し、暗号化が完了すると前記端末制御手段により前記暗号化情報が消去され、暗号を解くための情報を端末内から無くなることで、手元の携帯端末に記憶されたホスト装置への接続手順を含むデータを暗号化して参照不能にすると共に、これを復号化する為の復号化情報をホスト装置に保存することにより、安全にデータ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【請求項8】請求項1、3、4、5または6において、前記携帯端末の端末制御手段に前記ホスト装置から暗号化情報または制御コマンドが送信されたことを検出する機能と、前記検出を受けると前記データ記憶手段に記憶されたデータの漏洩防止処理をしている間、データ表示手段により後述するメッセージを表示する機能、前記読み出し専用記憶手段にホスト装置との接続処理を実行中であることを示すメッセージを記憶する機能を備えることで、第三者が携帯端末を取得して、ホスト装置を不正に利用する目的で接続操作を行い、接続処理が完了したとき、前記端末制御手段によりホスト装置から暗号化情報または制御コマンドが送信されたことが検出され、前記読み出し専用記憶手段から取り出したメッセージがデータ表示手段により第三者に提示され、表示されている間に漏洩防止処理が行われることで、実際には接続が完了していても、第三者に暗号化処理が実行されていることを認識させないことを特徴としたデータ漏洩防止シス

テム。

【請求項9】請求項1、3、4、5または6において、前記ホスト装置のホスト側通信手段が端末ID番号の照合機能に加えて、前記情報記憶手段から情報を取出す前に、前記携帯端末に対して特定の暗証番号の入力を求める機能と、前記入力された暗証番号が誤った事を計数し、予め設定された回数以上になると暗号化情報を携帯端末へ送信する機能を備えることで、携帯端末の所有者が何らかの事情により携帯端末を紛失し、前記携帯端末が第三者により取得されて、ホスト装置の前記情報記憶手段から情報が取出されるとき、第三者が特定の回数以上暗証番号の入力を間違えると自動的に前記携帯端末のデータ記憶手段に記憶されたデータと、前記データに含まれるホスト装置への接続手順を参照不能にして、データ記憶手段のデータとホスト装置内のデータの漏洩を防止できることを特徴とするデータ漏洩防止システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、携帯端末内部またはこの端末に接続されるデータ通信システムに記憶されたデータの漏洩防止システムに関する。

【0002】

【従来の技術】記憶装置内のデータが第三者へ漏洩することを防止する手段として、従来より何らかの操作をする前（例えばデータファイルへの接続）に利用者へ暗唱番号の入力を要求する方法や、データ自身の暗号化が用いられている。特に、携帯する事を前提とする端末には、オフィスで据置にして利用される端末には無い紛失や盗難といった危険性を持っているため、端末内のデータを守るために必ず上記の様なデータの保護手段が備わっている。

【0003】このようなシステムの例としては特開平1-126793号公報のようにICカードに記憶されたデータを守るために、同じ暗号キーを端末とICカードが持ち、相互に暗号化したデータを復号化して認証し合うことで同ICカードが正規端末で利用されている事を確認し、データの利用を許可するシステムや、特開平4-233647号公報のように利用者が入力する個人確認情報をICカードにおいて確認し、正規利用者であることが確認されるとホストコンピュータを利用できるシステムなどがある。

【0004】

【発明が解決しようとする課題】上記従来技術では、データの不正利用を防止する為に暗号キーや個人確認情報を用いている。

【0005】しかし、これら照合をする為のデータは、通常本体内またはICカード内の記憶デバイスに所有者が操作できないように記憶された上、書き換えが可能でも不用意にデータが失われないようにするために、記憶保持には電源を必要としないことが多い。よって、もし

も本体または本体とICカードと共に紛失したり、盗難に遭うなどした場合、第三者が故意に内部の記憶デバイスを取り出し、同デバイス内のデータを読み取る装置を使用すれば、照合用データ入手することが可能で、これはすなわち端末内のデータの漏洩だけではなく、この端末で接続できるホスト装置内のデータも漏洩する可能性が有ることを示しており、安全性の観点から不十分である。

【0006】また、紛失届けをホスト装置に出すことでのホスト装置内のデータを守ることは出来るが、この場合、端末内のデータを守ることが出来ない。

【0007】本発明の目的は、内部の記憶デバイスを取り出されるような場合でも、携帯端末内に記憶されたデータが漏洩するのを防止すること、紛失や盗難後でもデータ漏洩を防止出来るようにすること、またこの機能を必要に応じて所有者が簡単に解除できることにある。

【0008】

【課題を解決するための手段】本発明は、上記目的を達成するために、各端末の端末ID番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ID番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ID番号と、端末側での暗号化に使用する暗号化情報を記憶する暗号情報記憶手段と、照合された端末ID番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ID番号を照合する機能と、暗号化情報を携帯端末へ送信する機能を持つホスト側通信手段とを有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、ホスト装置と通信を開始する時に端末ID番号をホスト装置へ送信する機能と、暗号化情報を受信する機能を持つ端末側通信手段と、暗号化情報を消去する機能と、各携帯端末の端末ID番号を記憶する読み出し専用記憶手段と、暗号化処理をするための演算手段を持つ端末制御手段とを有する携帯端末を備える。

【0009】また、本発明は、各端末の端末ID番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ID番号とパスワードを照合する機能を持つ所有者通信手段と、端末側での復号化に使用する復号化情報を記憶する暗号情報記憶手段と、照合された端末ID番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ID番号を照合する機能と、復号化情報を携帯端末へ送信する機能を持つホスト側通信手段を有するホスト装置と、ホスト装置からの呼出しに対して端末ID番号をホスト装置へ送信する機能と、復号化情報を受信する機能を持つ端末側通信手段と、各携帯端末の端末ID番号を記憶

する読み出し専用記憶手段と、復号化処理をするための演算手段と持つ端末制御手段と、所有者用のデータとホスト装置から送信された復号化情報を記憶する書換え可能なデータ記憶手段と、を有する携帯端末を備える。

【0010】また、本発明は、各端末の端末ID番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ID番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ID番号と暗号化情報を消す消去コマンドを記憶する暗号情報記憶手段と、照合された端末ID番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ID番号を照合する機能と、消去コマンドを暗号情報記憶手段から取り出し携帯端末へ送信する機能を持つホスト側通信手段と有するホスト装置と、所有者用のデータと暗号化と復号化の為の暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、各携帯端末毎の端末ID番号を記憶する読み出し専用記憶手段と、日常動作ではデータ記憶手段内のデータを常に暗号化し、必要なときのみ復号化する演算手段を持つ端末制御手段と、ホスト装置と通信を開始する時に端末ID番号をホスト装置へ送信する機能と、暗号化情報の消去コマンドを受信する機能を持つ端末側通信手段と、消去コマンドを実行する端末制御手段とを有する携帯端末を備える。

【0011】また発明は、各端末の端末ID番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ID番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ID番号と、端末側での暗号化に使用する暗号化プログラムと暗号キーを記憶する暗号情報記憶手段と、照合された端末ID番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ID番号を照合する機能と、暗号化プログラムと暗号キーを携帯端末へ送信する機能を持つホスト側通信手段と有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化プログラムと暗号キーと、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、暗号化プログラムを消去する機能と、各携帯端末の端末ID番号と暗号キーを記憶する読み出し専用記憶手段と、暗号化プログラムにより暗号化処理をする演算手段を持つ端末制御手段と、ホスト装置と通信を開始する時に端末ID番号をホスト装置へ送信する機能と、暗号化プログラムを受信する機能を持つ端末側通信手段とを有する携帯端末を備える。

【0012】また、本発明は、各端末の端末ID番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ID番号とパ

スワードを照合する機能を持つ所有者通信手段と、暗号化処理を開始させる制御コマンドを発行するホスト制御装置と、照合された端末ID番号と、端末側での暗号化に使用する暗号キーを記憶する暗号情報記憶手段と、照合された端末ID番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ID番号を照合する機能と、暗号キーと制御コマンドを携帯端末へ送信する機能を持つホスト側通信手段とを有するホスト装置と、ホスト装置と通信を開始する時に端末ID番号をホスト装置へ送信する機能と、暗号キーと制御コマンドを受信する機能を持つ端末側通信手段と、所有者用のデータとホスト装置から送信された暗号キーと、ホスト装置との接続手順を記憶する書換え可能なデータ記憶手段と、暗号キーを消去する機能と、各携帯端末の端末ID番号を記憶する読み出し専用記憶手段と、ホスト装置から制御コマンドを受けて暗号化処理を開始する演算手段を持つ端末制御手段とを有する携帯端末を備える。

【0013】また発明は、各端末の端末ID番号と各端末の所有者へのパスワードを記憶した端末情報記憶手段と、公衆回線や一般加入回線を介して所有者と通信を行う機能と、その所有者が入力する端末ID番号とパスワードを照合する機能を持つ所有者通信手段と、照合された端末ID番号と、端末側での暗号化に使用する暗号化プログラムを記憶する暗号情報記憶手段と、照合された端末ID番号によって当該携帯端末を呼出す機能と、携帯端末から送信された端末ID番号を照合する機能と、暗号化プログラムを携帯端末へ送信する機能を持つホスト側通信手段と有するホスト装置と、所有者用のデータとホスト装置から送信された暗号化プログラムと、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、暗号化プログラムを消去する機能と、各携帯端末の端末ID番号と暗号キーを記憶する読み出し専用記憶手段と、暗号化プログラムにより暗号化処理をする演算手段を持つ端末制御手段と、ホスト装置と通信を開始する時に端末ID番号をホスト装置へ送信する機能と、暗号化プログラムを受信する機能を持つ端末側通信手段とを有する携帯端末を備える。

【0014】また発明は、各端末の端末ID番号を予め登録された端末情報記憶手段と、携帯端末から送信された端末ID番号を照合する機能と、端末から送信された復号化情報を受信するホスト側通信手段と、復号化情報と照合された端末ID番号を記憶する暗号情報記憶手段と有するホスト装置と、所有者用のデータと暗号化情報と、ホスト装置との接続手順を記憶した書換え可能なデータ記憶手段と、所有者が暗号化処理を要求すると暗号化情報の入力をデータ表示手段を介して所有者に促す機能と、暗号化情報を消去する機能と、各携帯端末の端末ID番号を記憶する読み出し専用記憶手段と、暗号情報がホスト装置に送信された後に暗号化処理をする演算手段を持つ端末制御手段と、データ記憶手段に記憶され

たデータを所有者に提示する為のデータ表示手段と、所有者が暗号化の要求と暗号化情報を入力する為のデータ入力手段と、ホスト装置と接続手順により通信を開始する時に端末ID番号をホスト装置へ送信する機能と、暗号化情報を復号化情報としてホスト装置へ送信する機能と、送信が終了したことを演算手段に通知する機能を持つ端末側通信手段とを有する携帯端末を備える。

【0015】

【作用】本発明では、携帯端末がホスト装置から送信される暗号化情報により、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号化情報を暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【0016】また、通信回線を介してホスト装置から暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【0017】また本発明では、携帯端末がホスト装置から送信される復号化情報により、内部に記憶した暗号化済みデータの復号化を行うので、復号化の為の情報を内部に持たない携帯端末でも通信回線を介して所有者の指示により簡単に暗号化を解除できる。

【0018】また本発明では、携帯端末が常に内部に記憶するデータの暗号化を行い、必要なときだけ暗号化に使用した情報を元に復号化を行うので、この暗号化情報を消去することにより、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【0019】また、通信回線を介してホスト装置から暗号化情報の消去を指示出来るので、端末が手元に無い状態でもデータが漏洩するのを防止できることになる。

【0020】また本発明では、携帯端末がホスト装置から送信される暗号化プログラムと暗号キーにより、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号化プログラムと暗号キーを暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【0021】また、通信回線を介してホスト装置から暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【0022】さらに、暗号化のためのプログラムを内蔵していない携帯端末でもデータの暗号化が可能となる。

【0023】また本発明では、携帯端末がホスト装置から送信される暗号キーと制御コマンドにより、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号キーを暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【0024】また、暗号キーと制御コマンドだけを通信回線を介してホスト装置から送信すればよいので、通信時間を短くでき、さらに通信回線を介して暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【0025】また本発明では、携帯端末がホスト装置から送信される暗号化プログラムと、端末内部に固定値として記憶されている暗号キーにより、内部に記憶しているデータの暗号化を行い、さらに暗号化に使用した暗号化プログラムを暗号化の終了で削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【0026】また、通信回線を介してホスト装置から暗号化処理を携帯端末に指示出来るので、端末が手元に無い状態でも暗号化処理を行い、データが漏洩するのを防止できることになる。

【0027】さらに、暗号化のためのプログラムのアルゴリズムを変更できるので、同じ暗号キーでも異なった暗号化が可能となる。

【0028】また本発明では、所有者が携帯端末内のデータを暗号化する為に暗号情報を端末に入力すると、暗号化処理を開始する前に暗号情報をホスト装置の記憶手段に記憶させ、その後端末内にあるホスト装置への接続手順を含むデータの暗号化を行い、暗号化の終了で暗号化情報を削除するので、たとえ第三者によって内部を分解されたとしてもデータを読み取ることは不可能になる。

【0029】また、暗号化の指示を手元の携帯端末から任意の時点で行えるので、紛失や盗難の可能性が有る場合に対してデータ漏洩を予防することが出来る。

【0030】

【実施例】以下、本発明を図示した各実施例によって説明する。

【0031】<第1実施例>図1は、本発明の第一実施例の携帯端末間のデータ漏洩防止システムの概念図で、図2は本システムで携帯端末がホスト装置と接続されるまでの概略図で、図3は本実施例の詳細な図である。

【0032】本実施例は、所有者が携帯端末を紛失、または盗難に遭った後を示したものである。

【0033】図1で、2は携帯端末、1は携帯端末2の所有者、3は携帯端末2のホスト装置であり、後述するように携帯端末2に関する情報や所有者に提供する情報のデータベースを備える。4は所有者1とホスト装置3との間を接続する公衆回線網、5はホスト装置3に接続された専用端末、6は携帯端末2とホスト装置3との間を接続する通信回線網であり、有線または無線方式の公衆または専用回線網である。7は携帯端末2を不正に利用しようとしている不正利用者、1501は携帯端末2が暗号化をするための暗号化情報である。

【0034】図2で、17は所有者1が携帯端末2により取り寄せることが出来る各種情報が蓄積されたデータベースで情報DB、902は通信回線網6を介してホスト装置3と接続する為の呼出し方法を示した接続手順、31は接続手順902により携帯端末2がホスト装置3と最初に接続されるゲート、1204は後述するROM1201に記憶された携帯端末2に固有の端末ID番号B、32は端末ID番号B1204を確認する第二のゲートで、ここで番号が確認されると携帯端末2がホスト装置3に接続される。また、904は所有者を認証するための所有者パスワードで、これが確認されると情報DB17を操作できる。

【0035】図3の携帯端末2では、101は所有者1が公衆回線網4または専用端末5でホスト装置3に入力する端末ID番号A、102は同じく所有者1がホスト装置3へ入力するパスワードA8はホスト装置3からの呼出しを受信し、後述する端末ID番号送信機能801によって端末ID番号で応答する機能と、ホスト装置3と通信回線網6を介してデータ送受信をする為の端末側通信手段、9は書換えが可能でかつ一旦記憶操作が行われた後は外部からの給電無しに各種データを保持できるデータ記憶手段、10はデータ記憶手段9に保持されたデータを所有者に提示するためのデータ表示手段、11は所有者がデータを入力する為のデータ入力手段、12は端末側通信手段8とデータ記憶手段9とデータ表示手段10とデータ入力手段11を制御する端末制御手段、1201は端末制御手段12にありデータの書き込みが一度だけ出来る読み出し専用記憶手段（以下ROM）、1202も端末制御手段12にあり暗号化計算を行う演算手段、1206は演算機能1202が暗号化計算を終了すると出力する信号で完了、1203は完了1206を受けるとデータ記憶手段9に記憶された暗号化情報1501を消去する消去機能、1205は消去機能1203がデータ記憶手段9へ出力する消去信号、801は端末ID番号B801をホスト装置3へ送信する端末ID番号送信機能、802は通信回線網6を介して送信された暗号化情報1501を受信してその誤りをチェックした後、データ記憶手段9へ入力する受信誤りチェック機能、901はデータ記憶手段9に記憶された所有者1の使う通常データ、903は暗号化をする前のデータで暗号化前データ、1206は演算手段1202で暗号化された暗号データである。

【0036】また、ホスト装置3では、13は携帯端末2と通信回線網6を介してデータ送受信をする為のホスト側通信手段、14は公衆回線網4または専用端末5を介して携帯端末2の所有者1と通信を行うための所有者通信手段、15は所有者通信手段14により入力される情報と暗号化に必要な暗号化情報1501を記憶する為の暗号情報記憶手段、1601は各端末のID番号を記憶したデータベースで端末ID番号DB、1602は各

端末の所有者に対するパスワードを記憶したデータベースでパスワードDB、1603はパスワードDB1602から端末ID番号A101で呼出されるパスワードB、16は端末ID番号DB1601とパスワードDB1602を記憶する端末情報記憶手段、1302は端末ID番号送信機能801から送信された端末ID番号B1204と所有者1が所有者通信手段14から入力した端末ID番号A101を照合する端末ID番号照合機能、1304は端末ID照合機能1302が照合出来た事を示す信号でID確認、1301はID確認1304を受けると暗号化情報1501を通信回線網6を介して携帯端末2へ送信する暗号情報送信機能、1303は端末ID番号A101によって携帯端末2を呼出す端末呼出し機能、1401は公衆回線網4または専用端末5から所有者1が入力した端末ID番号A101を受信し、これを端末情報記憶手段16へ入力し、後述するパスワード確認がされると端末ID番号A101を暗号情報記憶手段15へ入力するID番号受信機能、1402はパスワードDB1602からパスワードB1603を取り出し、後述するパスワード要求1403を所有者1へ送信し、所有者1からパスワードA102が入力されると、パスワードA102とパスワードB1603の照合を行い確認結果をID番号受信機能1401へ入力するパスワード確認機能、1403は端末ID番号A101の入力に対して所有者1を正規の利用者であることを認証する為のパスワードを要求する信号でパスワード要求、1404はパスワード確認機能1402がパスワードを確認出来たことを示す信号で確認である。

【0037】次に、本実施例の動作を、図1、図2、図3を用いて説明する。

【0038】まず本実施例で対象としているデータ通信システムでは図2に示すように、携帯端末2が情報DB17を操作するには、最初に接続手順902によりホスト装置3のゲート31と接続し、次にゲート32で端末ID番号B1204を入力し、番号が確認されると携帯端末が接続され、続いて所有者パスワード904を入力すると情報DB17と接続されるようになっている。

【0039】また、ホスト装置への接続のたびに所有者パスワード904を入力することは、通常の利用ではかえって煩わしい場合もあるので、この場合には接続手順902の中に所有者パスワード904も含めてしまうことも可能である。

【0040】つまり、携帯端末2は所有者1のプライベートな情報だけでなく、ホスト装置3への接続も可能な機能を備えており、第三者によって所有者パスワード904が破られ、利用されると損害が発生する可能性のある端末であり、接続手順に所有者パスワードが含まれるような場合は尚更である。

【0041】以下の説明は、所有者1が携帯端末2をいずれかで紛失したことに気付いたところで、図1に示す

ようにデータ漏洩防止の操作をするところから説明する。

【0042】そこで、所有者1は少しでも携帯端末2から情報が漏れることを防止するために、手近にある公衆回線網4またはホスト装置3の専用端末5からデータ漏洩防止の操作を行う。

【0043】すると、この操作ではまずホスト装置3が所有者通信手段14のID番号受信機能1401で、所有者1から入力された端末ID番号A101を受信し、これを端末情報記憶手段16へ入力する。端末ID番号A101を入力された端末情報記憶手段16は、端末ID番号DB1601とパスワードDB1602からこの端末ID番号A101の所有者1に登録されたパスワードB1603を取り出し、これをパスワード確認機能1402へ入力する。

【0044】パスワードB1603を入力されるとパスワード確認機能1402は、所有者1に対して公衆回線網4またはホスト装置3の専用端末5からパスワードの入力を促すパスワード要求1403を出力する。これに対して、所有者1がパスワードA102を入力すると、パスワード確認機能1402は先のパスワードB1603とパスワードA102を照合して、もし同じであることが確認できたら、すなわち、データ漏洩防止の操作をしている人物が、携帯端末2の正規の所有者であることを確認したら、これを示す信号、確認1404をID番号受信機能1401へ入力する。そして、確認1404を受けたID番号受信機能1401はこの端末が第三者に利用されることにより、データ漏洩の恐れのある端末として登録する為に、端末ID番号A101を暗号情報記憶手段15に記憶させる。

【0045】この後、ホスト装置3は自ら先に記憶した端末ID番号A101とホスト側通信手段13の端末呼出し機能1303と、通信回線網6により携帯端末2を呼出すか、または不正利用者7が携帯端末2を使ってデータ記憶手段9に記憶した接続手順902と、通信回線網6を介してホスト装置3を呼出すかすると、携帯端末2が端末制御手段12のROM1201に予め記憶している端末ID番号B1204を、端末側通信手段8の端末ID番号送信機能801によりホスト装置3へ送信し、一方、ホスト装置3ではホスト側通信手段13の端末ID番号照合機能1302が、暗号情報記憶手段15から端末ID番号A101を取り出し、携帯端末2から送信された端末ID番号B1204と照合を行う。

【0046】この照合で一致が確認されるとID確認1304が暗号情報送信機能1301へ入力され、暗号情報送信機能1301は暗号情報記憶手段15に記憶されている暗号化情報1501を通信回線網6を介して携帯端末2へ送信する。（なお、ホスト装置3に端末ID番号が登録されていないとき、つまり通常の場合は暗号化情報1501に代って所有者パスワード904の入力が

求められることになる。）携帯端末2は端末側通信手段8の受信誤りチェック機能802で暗号化情報1501を受信し、誤りの有無を確認した後、データ記憶手段9に記憶する。暗号化情報1501が記憶されると、端末制御手段12はデータ記憶手段9に記憶されている、通常データ901と接続手順902を暗号化前データ903として取出し、これらを演算手段1202へ入力する。

【0047】データを入力された演算手段1202は、先に記憶された暗号化情報1501をデータ記憶手段9から取出し、これに基づいて入力されたデータを暗号化する。

【0048】暗号化されたデータは暗号データ1206となり、データ記憶手段9へ入力され、暗号化前データ903に上書きして記憶される。そして、すべての通常データ901と接続手順902の暗号化が終了すると、演算手段1202は完了1206を消去機能1203へ入力し、消去機能1203は消去信号1205を発生してデータ記憶手段9に記憶された暗号化情報1501を消去するので、以後携帯端末単独では暗号化されたデータを元に戻すことは不可能になる。

【0049】本実施例によれば、携帯端末を紛失後でも手近な通信手段を使ってホスト装置に紛失した事を登録すれば、後は携帯端末とホスト装置との接続が行われることにより、以後携帯端末内に記憶された所有者のプライベートな情報も、ホスト装置への接続手順も参照することが出来なくなるので、データの漏洩による損害を最小限に出来る。

【0050】もちろん、接続をする前に不正利用者7が接続情報902を何らかの手段によって取出すこともあり得るが、ホスト装置と通信をするには端末ID番号B1204が必要である為、接続手順だけを不正利用者7が用意した第二の携帯端末に記憶させても通信は出来ず、またさらに何らかの方法で端末ID番号Bも取出して通信を確立したとしても、ホスト装置3からは暗号化情報1501が送信されるので、この第二の携帯端末のデータ記憶手段に記憶された内容も暗号化されることになる。よってこの場合、漏洩するデータは携帯端末2に記憶されていたデータに限られることになり、ホスト装置3にある情報DB17が利用されることはない。

【0051】なお、図示しないが所有者1が紛失したことに気が付くのが遅くなり、まだデータ漏洩防止の操作を行っていない場合でも、不正利用者7が情報DB17への接続で、ホスト装置3から要求される所有者パスワード904の入力を、予めホスト装置3で決められている回数を越えて失敗したかどうかを判断するようにして、たとえ所有者1からの操作が無くても上記の暗号化処理を自動的に行うようにしてもよい。

【0052】さらに、すでに所有者1によりデータ漏洩防止の操作がなされているときに、不正利用者7がホス

ト装置3への接続を試みると、上記のごとく携帯端末2では暗号化処理が行われるが、このときデータ表示手段10には既にホスト装置3との接続は完了していても、例えば「ただ今ホスト装置への接続処理中です」と言ったメッセージを表示し続け、暗号化処理中であることを悟られないようにすることで、犯罪を目的として操作したのではない不正利用者7に不要な不快感を与えることのないようにもできる。

【0053】また、暗号化情報1501を暗号化プログラムと暗号化時の係数となる暗号キーとすれば、図4に示すように暗号情報記憶手段15に暗号化プログラム1502と暗号キー1503を予め記憶しておき、これらを暗号化情報1501として送信し、携帯端末2ではデータ記憶手段9がこれらを記憶して、演算手段1202が暗号化プログラム1502を実行し、暗号キー1503を係数として暗号化前データ903を暗号データ1206に変換するようにすれば、暗号化のためのプログラムを内蔵していない携帯端末でもデータの漏洩を防止できることになる。

【0054】また、これに端末ID番号による機種判別を加えれば、機種毎の暗号化プログラムをホスト装置が用意することも可能である。

【0055】さらに、図示しないが暗号化プログラムを内蔵している場合には、暗号化情報1501として暗号キー1503と暗号化プログラムに起動を掛けるための制御コマンドを用いることも可能で、この場合には携帯端末2が暗号キー1503と制御コマンドといった簡単なデータを受信するだけで済むので接続時間が短くなり、それだけ通信費が安くなる。

【0056】またさらに、上記とは逆に暗号キーを既に内蔵している場合には、暗号化情報1501として暗号化プログラム1502を用いることも可能で、この場合には多少接続時間は長くなるが、同じ暗号キーでも暗号化的アルゴリズムを自由に変更できるので、常に最新方式の暗号化を所有者1に提供できるとともに、万が一プログラムにバグがある場合にも対応が簡単にできるようになる。

【0057】<第2実施例>図5は、本発明の第二実施例のデータ漏洩防止システムにおける、データの復号化動作の説明図である。

【0058】図5で、1504は携帯端末2が暗号データ1206を復号化するために使う復号化情報、1207は演算手段1202が暗号データ1206を復号化した復号化後データである。また、第一実施例と異なり、ID番号受信機能1401にはホスト側通信手段13へ端末ID番号A101を出力する機能、暗号情報送信機能1301にはID確認1304を受けると復号化情報1504を通信回線網6を介して携帯端末2へ送信する機能を有する。

【0059】次に本実施例の動作を図5を用いて説明す

る。なお本実施例では、携帯端末2のデータ記憶手段9には既に暗号化されたデータ、つまり暗号データ1206として記憶されており、所有者1がこれを復号化したいと思っている場合とする。

【0060】まず、所有者1は第一実施例と同様に手近な公衆回線網4または専用端末5からホスト装置3を呼び出し、端末ID番号A101を入力する。すると、ホスト装置3からパスワード要求1403があり、これに対してパスワードA102を入力すると、所有者通信手段14で照合がなされ、確認されると端末ID番号A101はホスト側通信手段13の端末呼出機能1303へ入力される。

【0061】そして端末呼出機能1303が通信回線網6を介して、端末ID番号A101で携帯端末2を呼び出すと、端末からこれに対する応答として端末ID番号B1204が端末ID送信機能801と通信回線網6を介して返送されるので、これを受信したホスト側通信手段13は端末ID番号照合機能1302で、端末ID番号A101と端末ID番号B1204の照合を行い、正しく照合がされるとID確認1304が暗号情報送信機能1301に入力される。

【0062】すると、ID確認1304を受けた暗号情報送信機能1301は、暗号情報記憶手段15に予め記憶していた復号化情報1504を通信回線網6を介して携帯端末2へ送信するので、携帯端末2はこれを端末側通信手段8で受信し、受信誤りチェック機能802で確認した後、データ記憶手段9に記憶する。

【0063】復号化情報1504が記憶されると、端末制御手段12の演算手段1202がデータ記憶手段9から暗号データ1206と復号化情報1504を取り出し、復号化処理を実行して復号化後データ1207に変換し、暗号化データ1206に上書きして記憶する。

【0064】以上の様に本実施例によれば、携帯端末2をデータ漏洩から守る為に行なった暗号化処理を手近な通信手段から簡単にいつでも解除することが可能になる。

【0065】また、復号化の情報が第三者には簡単に操作できないホスト装置に記憶されているので、所有者に情報を覚える煩わしさを持たせずに安全にデータを守ることが出来る。

【0066】なお図示はしないが、ここで復号化情報1504は第一実施例の図4の場合に対応して、復号化プログラムと暗号化に使った暗号キーとともに、また端末が暗号キーを内蔵しているときには復号化プログラムだけとすることも可能で、さらに端末ID番号により携帯端末の種類を特定できれば、機種毎に対応したプログラムを送信することも第一実施例と同様に可能になることは容易に想像できることである。

【0067】<第3実施例>図6は、本発明の第三実施例のデータ漏洩防止システムにおける、データの暗号化動作の説明図である。

【0068】図6で、1505は携帯端末2のデータ記憶手段9にある暗号化情報1501を端末制御手段12に消去するように命令する為の消去コマンド、1305はID確認1304を受けて消去コマンド1505を携帯端末2へ送信する消去コマンド送信機能である。

【0069】また、第一実施例と異なり、端末制御手段12の消去機能1203は消去コマンド1505を受けると起動する機能、演算手段1202は暗号化情報1501にある情報により暗号化と復号化の両方を実行する機能を有する。

【0070】本実施例が第一実施例と異なる点は、携帯端末が暗号化と復号化の機能を予め内蔵しており、入力手段から入力されるか、内部の演算によって得られたデータを必ず暗号化してから記憶手段に記憶させ、記憶されたデータを所有者に提示するなど必要なときだけ復号化する機能を有し、万が一の場合には暗号化と復号化の処理で使用する暗号化情報を消去することが可能な点にある。

【0071】次に、本実施例の動作を図6を用いて説明する。なお、本実施例も第一実施例と同様に、所有者1が携帯端末2をいざれかで紛失したことに気付いたところであるとする。

【0072】そこで、所有者1が第一実施例と同様に手近にある公衆回線網4またはホスト装置3の専用端末5からデータ漏洩防止の操作を行うと、端末ID番号A101の入力に続いてパスワード要求1403を受け、パスワードA120を入力すると端末ID番号A101が暗号情報記憶手段15に記憶される。

【0073】この後も第一実施例と同様に、ホスト装置3から携帯端末2を呼出すか、または不正利用者7が接続手順902によりホスト装置3を呼出すかすると、端末ID番号照合機能1302により端末ID番号の照合がなされ、一致が確認されると、暗号情報記憶手段15に記憶されている消去コマンド1505が取出され、消去コマンド送信機能1305がこのコマンドを通信回線網6を介して携帯端末2へ送信する。

【0074】一方、消去コマンド1505を受信した端末側通信手段8は、同コマンドを端末制御手段12の消去機能1203へ入力する。そして、消去機能1203が起動して消去信号1205をデータ記憶手段9へ入力すると、暗号情報1501が消去されるので、以後携帯端末単独では暗号化されたデータを元に戻すことは不可能になる。

【0075】本実施例によれば、携帯端末内のデータは既に暗号化されているので、暗号化処理のための時間が不要であり、紛失後でも手近な通信手段を使ってホスト装置に紛失した事を登録すれば、後は携帯端末とホスト装置との接続が行われることにより、携帯端末内に記憶された所有者のプライベートな情報も、ホスト装置への接続手順も瞬時に参照することが出来なくなるので、デ

ータの漏洩による損害を最小限に出来る。

【0076】また本実施例の場合ホスト装置から送信するデータは暗号情報を消去させるコマンドだけなので、全く機種の異なる携帯端末でも同コマンドの仕様だけ規定されていれば、ホスト装置側で機種別対応をしなくても、上記のようにデータの漏洩防止を図ることが可能になる。

【0077】<第4実施例>図7は、本発明の第四実施例のデータ漏洩防止システムにおける、データの暗号化動作の説明図である。

【0078】図7で、1102は所有者1がデータ入力手段11から入力した暗号化情報、1101は所有者1が携帯端末2に対して内蔵するデータを暗号化するよう命じる暗号化要求、1208は暗号化情報1102の入力を所有者1に要求する暗号情報入力要求、1209は端末側通信手段8にホスト装置3の呼出しと暗号化情報1102の送信を命じる暗号化開始指示、803はデータ記憶手段9に記憶された暗号化情報1102をホスト装置3へ送信する復号化情報送信機能、804は暗号化情報1102の送信が完了したことを演算手段1202へ通知するための送信終了、1504は暗号化情報1102と同じ情報で復号化のためにホスト装置3に記憶された復号化情報、1306は復号化情報1504を通信回線網6を介して受信して、ID確認1304が端末ID番号照合機能1302から出力されると、暗号情報記憶手段15に端末ID番号B1204と関連付けて記憶される復号化情報受信機能である。また、端末制御手段12に暗号化要求1101を受けると暗号情報入力要求1208をデータ表示手段10を介して所有者1に提示する機能と、暗号化情報1102の入力を受けると暗号化開始指示1209を出力する機能を有する。

【0079】本実施例が第一実施例と異なる点は、所有者が携帯端末を紛失した後にデータ漏洩防止の操作をするのではなく、紛失や盗難の可能性に対して予めデータ漏洩の防止をする点にある。

【0080】次に、本実施例の動作を図7を用いて説明する。ここでは、例えば所有者1が空港で手荷物を預ける際に、万が一の場合を考慮して手元にある携帯端末2内のデータを暗号化させようとしているとする。

【0081】まず、所有者1はデータ入力手段11から暗号化要求1101を入力する。すると、端末制御手段12から暗号情報入力要求1208がデータ表示手段10を介して所有者1に提示される。所有者1がこの要求に対して暗号化情報1102をデータ入力手段11から入力すると、端末制御手段12から端末側通信手段8に暗号化開始指示1209が入力される。指示を受けた通信手段は、接続手順902によって通信回線網6を介してホスト装置3と接続を行い、端末ID番号送信機能801により端末ID番号B1204の送信を行い、また復号化情報送信機能803によって暗号化情報1102

を復号化情報1504としてホスト装置3へ送信する。

【0082】一方、端末ID番号B1204を受信したホスト装置3では、端末ID番号照合機能1302で端末ID番号B1204が端末ID番号DB1601に登録されているか否かを確認し、登録されている場合にはID確認1304を復号化情報受信機能1306に入力し、端末ID番号B1204を暗号化情報記憶手段15に記憶させる。そして復号化情報受信機能1306は受信した復号化情報1504を先の端末ID番号B1204と対応させて記憶する。

【0083】また、復号化情報1504の送信を完了した携帯端末2では、端末側通信手段8が演算手段1202に暗号化処理を開始させる為に送信終了804を入力し、演算手段1202は第一実施例と同様に暗号化情報1102により暗号化前データ903を暗号データ1206へ変換し、データ記憶手段9へ入力して暗号化前データ903に上書き記憶する。そして、すべての通常データ901と接続手順902の暗号化が終了すると、演算手段1202は完了1206を消去機能1203へ入力し、消去機能1203は消去信号1205を発生してデータ記憶手段9に記憶された暗号化情報1501を消去するので、以後携帯端末単独では暗号化されたデータを元に戻すことは不可能になる。

【0084】本実施例によれば、携帯端末内のデータを損害が生じる前に、しかも所有者が望むときに予め暗号化することが出来るので、手荷物が盗難に遭うような事があってもデータが漏洩する恐れがなくなり、安心して預けることが出来る。

【0085】また、本実施例と第二実施例を組合せれば、本実施例で示すように暗号化した後、任意の時点で所有者が第二実施例のように復号化をホスト装置に依頼することでデータを回復できるといった使い勝手を実現でき、この場合復号化に使用する情報は暗号化されてい

る間、ホスト装置に保持されるので第三者がこれを取出すことは困難であり、データ漏洩に対する安全性が高いシステムを提供できる。

【0086】なお、データ記憶手段9は、フラッシュROMやEEPROMといった半導体デバイス、またはハードディスクや光磁気ディスクと言ったストレージデバイスであってもよい。

【0087】また、通信回線網6を介して端末とホスト装置を接続する手段にはセルラー無線、パーソナル・ハンディフォン・システム(PHS)、無線LAN、有線LANなど考えられる。

【0088】

【発明の効果】本発明によれば、携帯端末の所有者は端末の紛失や盗難に伴うデータ漏洩を最小限にとどめることができになる。また、そのための操作も手近な通信手段を用いてホスト装置に依頼するだけであり、所有者に負担を感じさせない安心感を提供できる。

【図面の簡単な説明】

【図1】本発明の概略の説明図。

【図2】本発明の携帯端末とホスト装置の接続の説明図。

【図3】本発明の第一実施例の説明図。

【図4】本発明の第一実施例の補足説明図。

【図5】本発明の第二実施例の説明図。

【図6】本発明の第三実施例の説明図。

【図7】本発明の第四実施例の説明図。

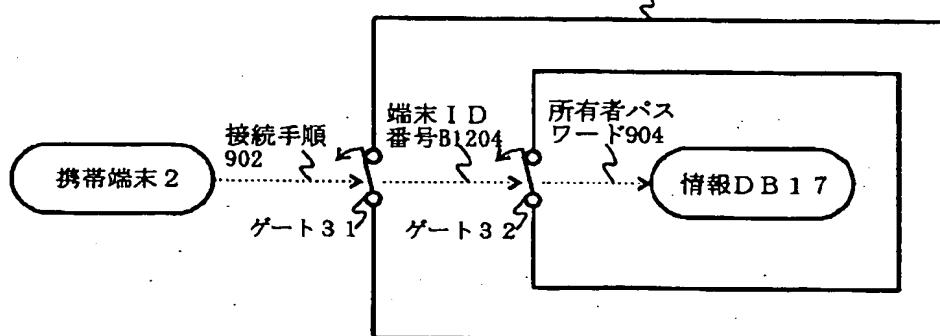
【符号の説明】

1…所有者、2…携帯端末、3…ホスト装置、4…公衆回線網、5…専用端末、6…通信回線、7…不正利用者、8…端末側通信手段、9…データ記憶手段、12…端末制御手段、13…ホスト側通信手段、14…所有者通信手段、15…暗号情報記憶手段、16…端末情報記憶手段。

【図2】

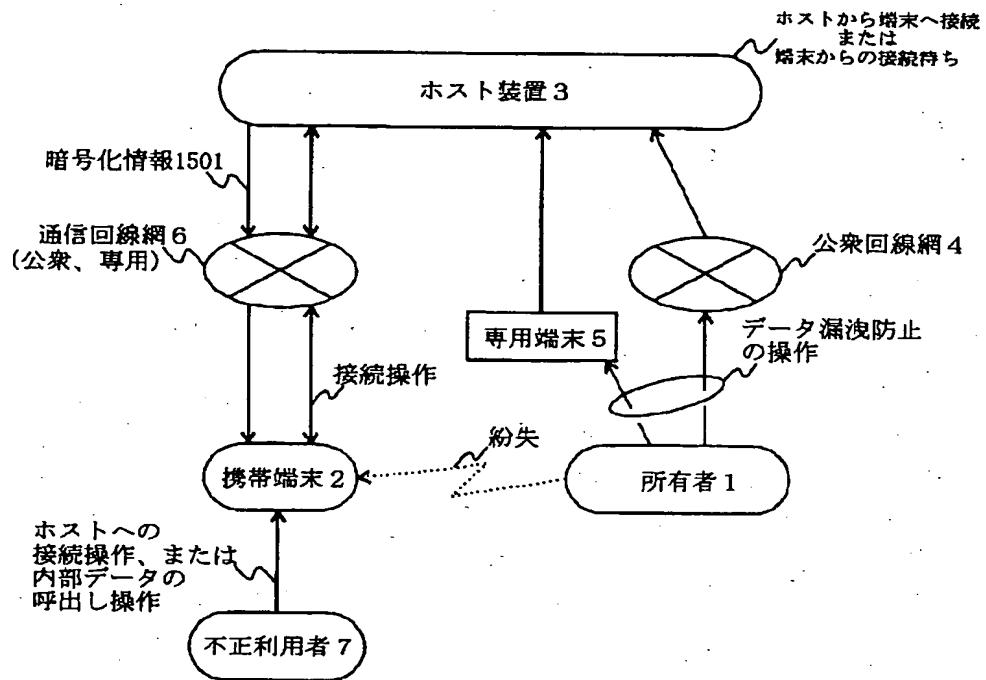
図2

ホスト装置3



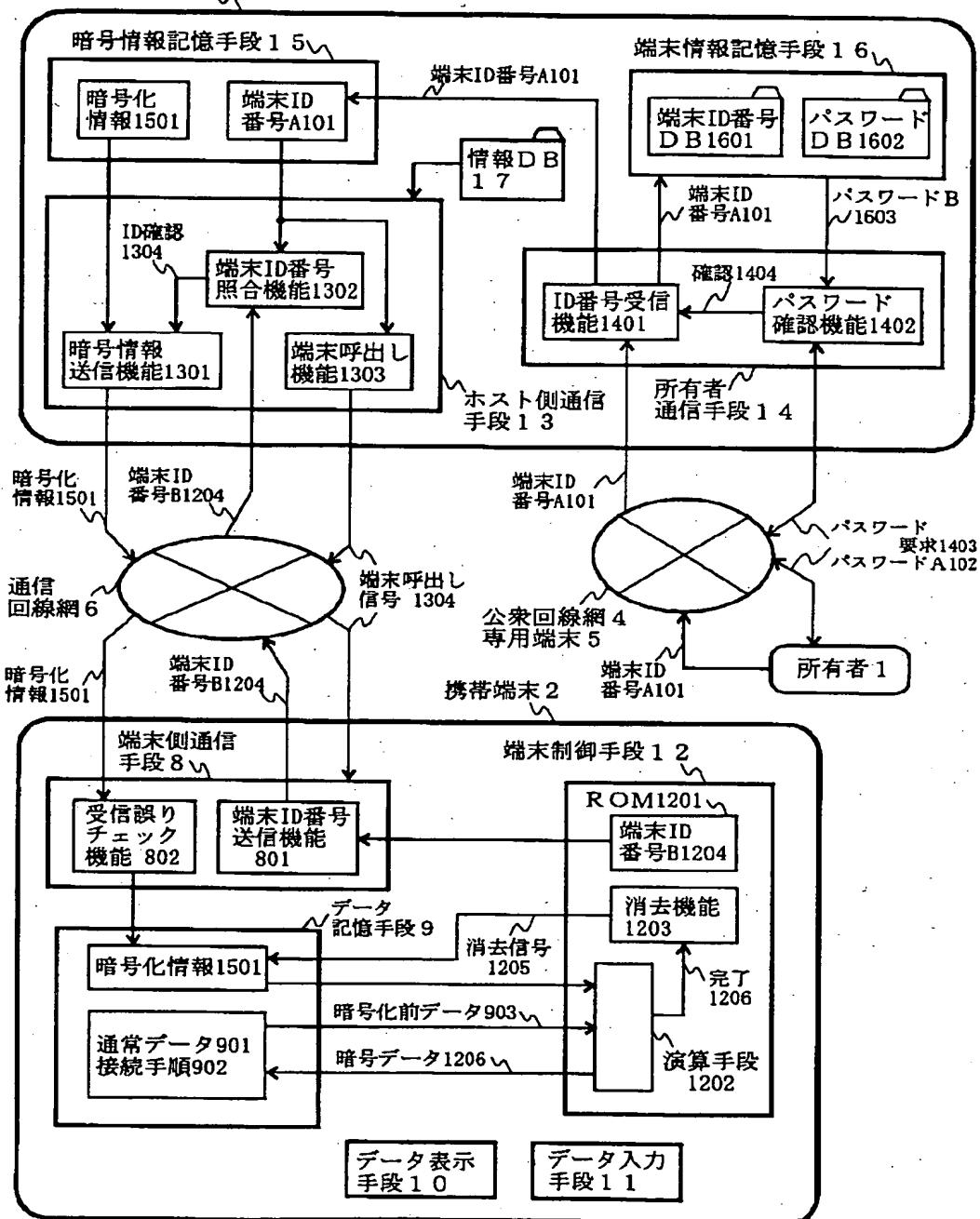
【図1】

図1



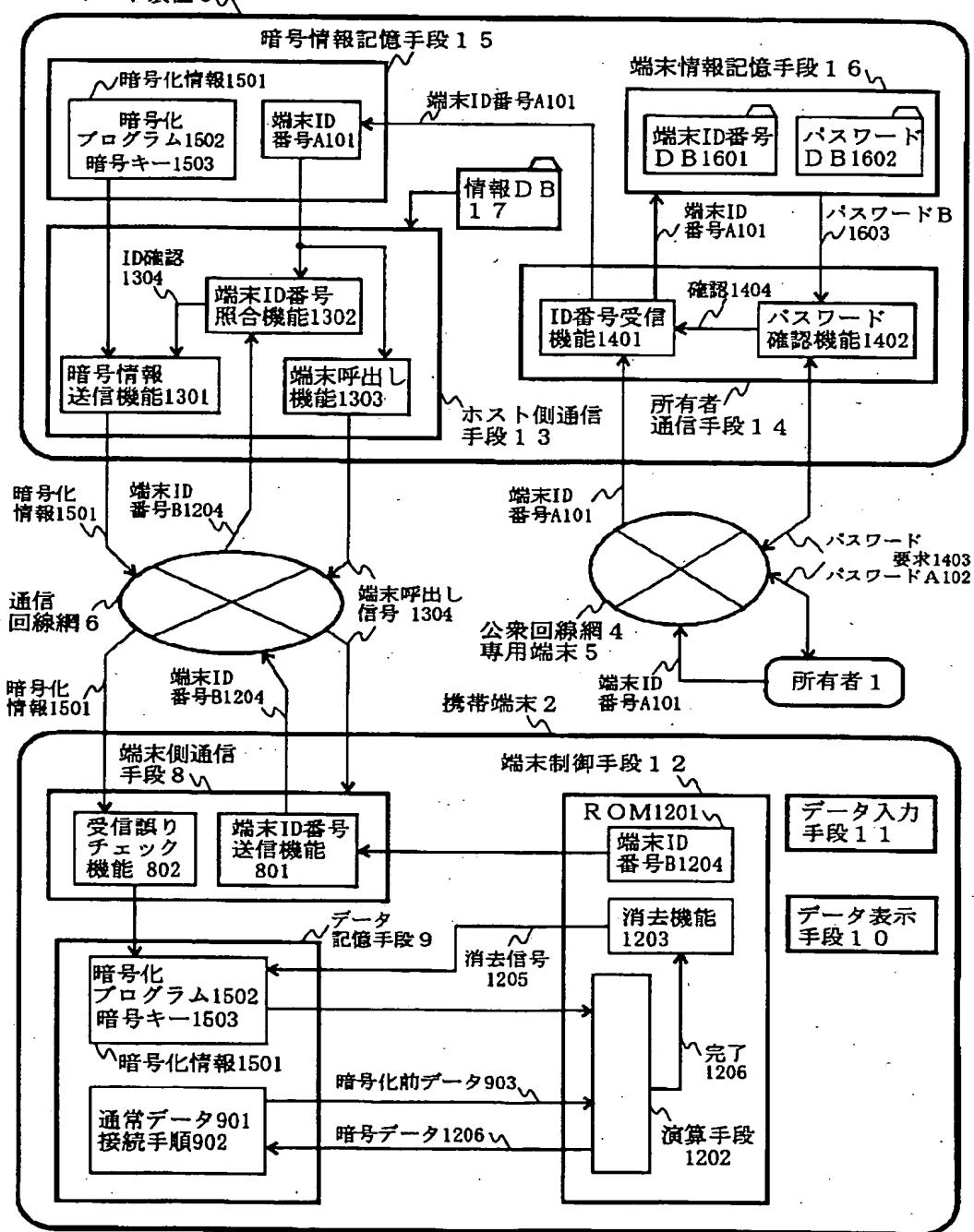
〔図3〕

3



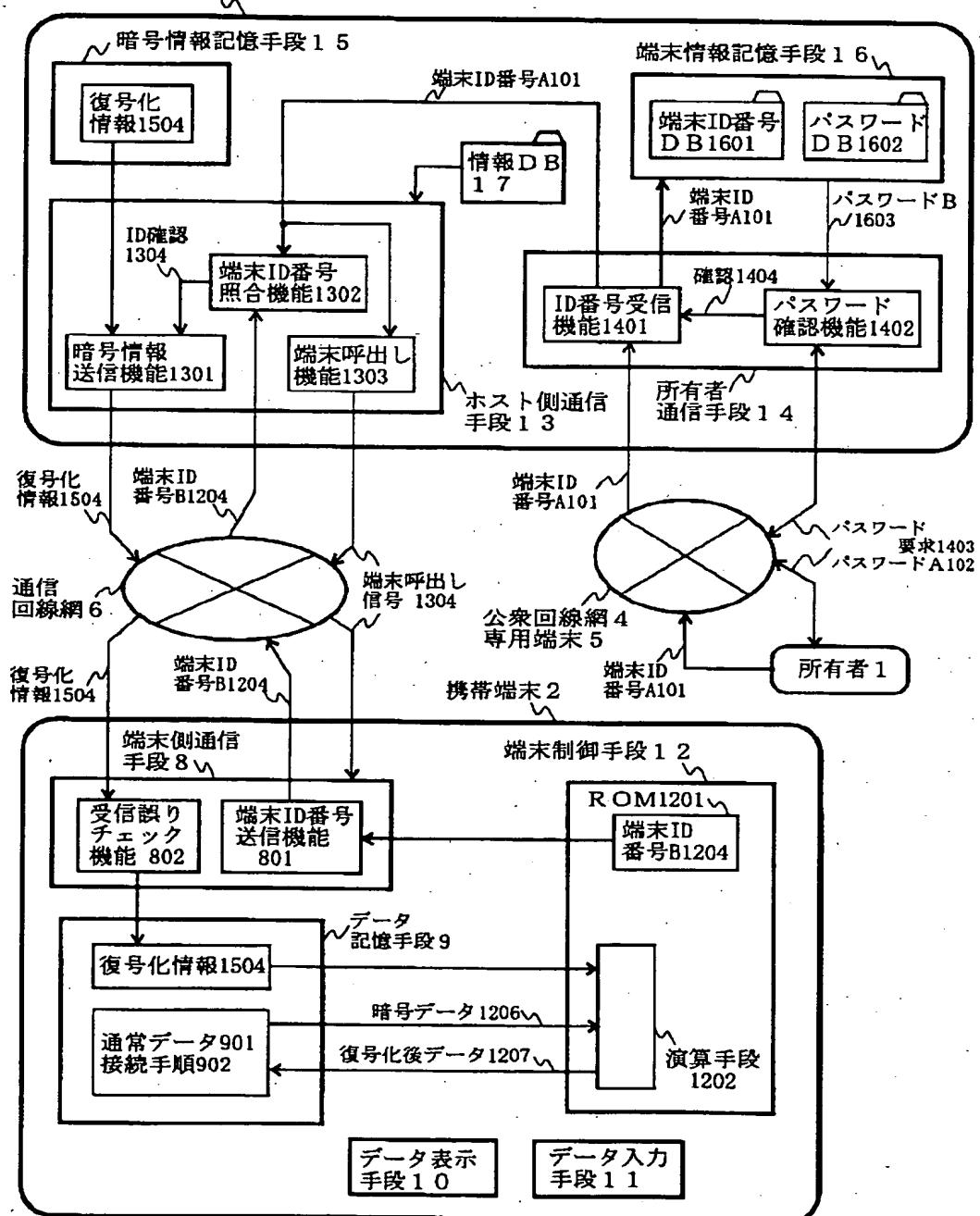
【图4】

☒ 4



【図 5】

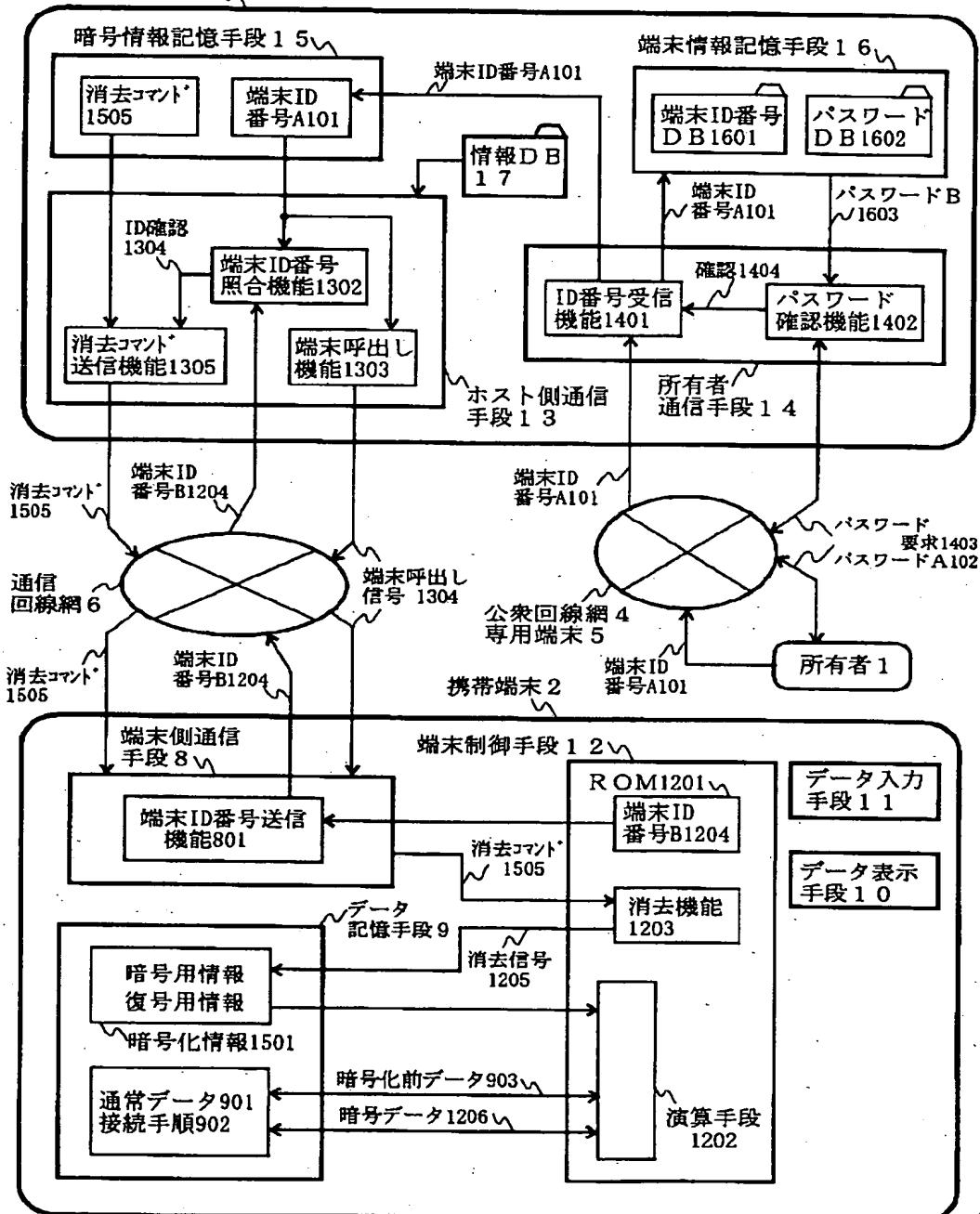
図 5



【図 6】

ホスト装置 3

図 6



【図7】

